# VVSG Security Overview

## Presentation for the Standards Board

**Dr. Ronald L. Rivest**
**John P. Wack**

**August 24, 2005**
**National Institute of Standards and Technology**
**http://vote.nist.gov**

# Topics

- Overview of new security material
- Software Distribution
- Setup Validation
- Wireless
- VVPAT

# Overview

Two major changes to VSS in security area:

1. Chapter 6 - Security
    1. Software Distribution/Setup Validation requirements
    2. Wireless telecommunications requirements
    3. VVPAT requirements - optional
2. Appendix D - new - informative IDV requirements

# Software Distribution and Setup Validation

- Software Distribution goal is to ensure correct code has been distributed w/o modification
- Setup Validation goal is to verify system is in proper state before being used
  - Requirements for presence of certified software
  - Requirements for verifying absence of other software

# Important!

- Voting system defined as being composed of multiple systems including
  - Polling place systems
  - Central count/aggregation systems
  - EMS

# Software Distribution Requirements

- Use of FIPS approved algorithms/modules for digital signatures and hashes and cryptographic modules in voting system
- Vendor shall document use of all software to be installed on the voting system including 3rd party software such as OS, drivers
- Testing lab witnesses final build

# Software Distribution Requirements

- Use of NIST National Software Reference Library (NSRL) as a repository for voting system binaries, hashes, and digital signatures - including COTS
- All voting system software distributed on read-only media (write once)
- Voting system shall provide means to verify that no unauthorized software is present on the voting equipment and that the authorized software has not been modified

# Setup Validation Requirements

- Vendor shall include method for verifying that correct software has been loaded and system is in proper initial state
- Should be possible to perform w/o use of software on the voting system
- Shall be able to be performed using COTS or 3rd party

# Setup Validation Requirements

- Voting system shall provide read-only external interface to inspect voting system software
- It shall be protected against tampering
- It shall be disabled during voting
- It shall provide physical indication when enabled/disabled
- It SHOULD provide direct read-only access to voting system software without the use of that software

# Wireless

- **Introduces severe risk and should be approached with extreme caution**
- Wireless presents opportunity for intruder access and denial of service
- Essential to protect data and access
- Important to understand threats and risks before justifying its use

# What is Affected

- Wireless includes radio frequency (RF), infrared (IR), microwave
- Covers
  - WiFi – 802.11x protocols
  - Bluetooth (used to connect to a modem for example)
  - IR (used to connect to cards, printers, etc)
- Does not cover modems in voting systems that connect to switch telephone network
- The wireless requirements currently affect relatively few (2) voting systems

# Wireless Requirements

- Wireless must follow at least the requirements of the existing telecommunications section in the 2002 VSS
- Vendor must document
  - how wireless is employed
  - how threats are mitigated
  - the rationale for its use
- Test labs must perform open review or use qualified expert
- In some cases wireless denial of service cannot be prevented, therefore alternatives must be available or the voting system can be rendered non-functional

# Wireless continued

- Must be able to be turned off when not used, must require voting official confirmation when turned on
- Wireless traffic must be encrypted and authenticated using FIPS 140-2
- Capability to xmit unencrypted/unauthenticated traffic shall not exist

# Wireless continued

- Voting system must resist denial of service attacks
- Wireless shall not be a single point of failure for voting system
- Alternatives to wireless must be provided in voting system
- Infrared wireless (line of sight, no built-in security) must be shielded to prevent escape of the signal

# VVPAT Requirements

- EAC asked TGDC to address VVPAT requirements for states considering its usage
- Optional in VVSG
- VVPAT system consists of DRE that stores electronic records plus printer plus verification capability

# VVPAT continued

- Based on enacted state legislation and CA standard
- Codifies record formats, security, usability and accessibility concerns
- Emphasizes machine/printer reliability
- Emphasizes usefulness of paper record in comparisons with electronic record
- Addresses usability for election officials when auditing paper and electronic records
- Emphasizes voter privacy in storage of paper record

# VVPAT Requirements Areas

- Display and Print a Paper Record
- VVPAT Voting Station Usability & Accessibility
- Approve or Spoil the Record
- Preserve Voter Privacy & Anonymity
- Electronic & Paper Record Structure
- Equipment Security & Reliability

# Usability & Accessibility

- Both records must be positioned to be easily viewable by voter
- Records must be structured so as to be easily compared by voter
- Clear instructions attached to voting station
- Paper record printed in any alternative languages
- Accessible voting station SHOULD enable sight-impaired to perform verification

# Privacy & Anonymity

- Records created and stored so as to preserve voter privacy
- Privacy preserved for paper records printed in any alternative languages
- Voter cannot leave with paper unless paper cannot reveal how voted
- Accessible voting station to maintain privacy if ballot box required and voter unable to manually handle paper

# Record Structure Requirements

- Both records structured so as to be easily and accurately compared
- Must contain election and other useful information
- Must be linked via a unique identifier
- Ideally, digital signatures used to link with specific voting system

# Record Structure Requirements

- Able to be exported in common format for easy analysis
- Paper record able to be machine read
- Barcode permissible on paper record if open format
- Vendor must document process for comparing electronic records to corresponding paper records

# Implications of Record Format

- Records must be easily and quickly compared and used in audits
- Interoperability of exported record format across all voting systems
- Digital signatures on records will provide trace back to specific voting system
- Unique ids used in audits estimated to greatly increase accuracy of results